

1

## CLAIM AMENDMENTS

2

3

### Claim Amendment Summary

4

5

#### **Claims pending**

6

- At time of the Action: Claims 1-15 and 18-35.
- After this Response: Claims 1-15, 18-26, and 28-35.

7

**Canceled or Withdrawn claims:** 27.

8

9

**Amended claims:** 1, 8, 18, 23, 24, 28, and 29.

10

11

**New claims:** none.

---

12

13

### Claims:

14

15

1. **(CURRENTLY AMENDED)** A method for accommodating a  
16 legacy application, the legacy application having provisions for a low-level  
17 credential authorization model which employs username-and-password  
18 based authorization, the method comprising:

19 obtaining a request for a high-level credential from a legacy  
20 application, wherein a high-level credential authorization model does not  
21 employ username-and-password based authorization;

22 marshalling the requested high-level credential, the marshalling is  
23 characterized by converting a description of the high-level credential into a  
24 format recognizable as a low-level credential by the legacy application  
25 employing a low-level credential authorization model;

returning the marshaled credential to the legacy application.

1  
2. (ORIGINAL) A method as recited in claim 1 further  
3 comprising, after the obtaining, seeking the requested credential in a  
4 database of credentials.

5  
6. 3. (ORIGINAL) A method as recited in claim 1, wherein a high-  
7 level credential is a credential selected from a group composed of X.509  
8 Certificates and bio-metrics.

9  
10. 4. (ORIGINAL) A method as recited in claim 1, wherein the  
11 marshaled credentials appear to be a conventional username/password pair  
12 to the legacy application.

13  
14. 5. (ORIGINAL) A method as recited in claim 1, wherein  
15 marshalling comprises:

16. obtaining the requested high-level credential;  
17. pickling the requested high-level credential to generate a low-level  
18 credential that represents the requested high-level credential while  
19 appearing to be a conventional username/password pair to the legacy  
20 application.

21  
22. 6. (ORIGINAL) A method as recited in claim 1, wherein the  
23 legacy application never has access to the high-level credential.

1           7.     **(ORIGINAL)** A computer-readable medium having computer-  
2 executable instructions that, when executed by a computer, perform a  
3 method as recited in claim 1.

4

5           8.     **(CURRENTLY AMENDED)** In a computing environment  
6 where processes have a provision for low-level credentials but have no  
7 provision for high-level credentials, wherein a provision for low-level  
credentials employs username-and-password based authorization while a  
provision for high-level credentials does not employ username-and-  
password based authorization, a method for accommodating such processes  
10 comprising:

11           obtaining a request for a credential from a process, wherein the  
12 requested credential is a high-level credential, which is not username-and-  
13 password based;

14           retrieving the requested credential from a database;

15           converting the requested high-level credential into a format  
16 approximating a low-level credential and representative of the requested  
17 high-level credential;

18           returning the converted credential to the process.

1           9.     **(ORIGINAL)** A method as recited in claim 8, wherein a high-  
2 level credential is a credential selected from a group composed of X.509  
3 Certificates and bio-metrics.

4

5           10.   **(ORIGINAL)** A method as recited in claim 8, wherein the  
6 converted credentials appear to be a conventional username/password pair  
7 to the process.

8

9           11.   **(ORIGINAL)** A method as recited in claim 8, wherein the  
10 process never has access to the high-level credential.

11

12          12.   **(ORIGINAL)** A computer-readable medium having computer-  
13 executable instructions that, when executed by a computer, perform a  
14 method as recited in claim 8.

15

16          13.   **(ORIGINAL)** A method for authenticating a user to a  
17 network, the method comprising:

18           obtaining a request for a credential to authenticate the user to access  
19 a resource within the network, wherein the resource requires an appropriate  
20 credential before the user may access the resource;

21           locating the appropriate credential;

22           returning the appropriate credential to the resource within the  
23 network, so that the resource allows the user to access such resource;

1           wherein the obtaining, locating, and returning are performed without  
2 user interaction so that the user need not be aware that such steps are being  
3 performed.

4

5       **14. (ORIGINAL)** A method as recited in claim 13 further  
6 comprising repeating the obtaining, locating, and returning for a different  
7 network that is authenticated using a different credential.

8

9       **15. (ORIGINAL)** A computer-readable medium having computer-  
10 executable instructions that, when executed by a computer, perform a  
11 method as recited in claim 13.

12

13       **16. (CANCELED)**

14

15       **17. (CANCELED)**

421 West Riverside, Suite 500  
Spokane, WA 99201  
P: 509.324.9256  
F: 509.323-8979  
[www.leehayes.com](http://www.leehayes.com)

**lee&hayes**

1           **18. (CURRENTLY AMENDED)**

A credential management

2 architecture, comprising:

3           a trusted computing base (TCB) that has full access to persisted  
4 credentials, the TCB being configured to interact with an untrusted  
5 computing layer (UTCL) that accesses the persisted credentials via the  
6 TCB;

7           the TCB comprises:

8           a credential management module configured to receive  
9 requests from the UTCL for a high-level credential for a resource,  
10 the high-level credential being associated with a user and not being  
11 username-and-password based authorization;

12           a credential database associated with the user, wherein  
13 credentials are persisted within the database;

14           the credential management module being configured to  
15 retrieve credentials from the database.

16           **19. (PREVIOUSLY PRESENTED)**

An architecture as recited

17 in claim 18, wherein credential management module is further configured  
18 to marshal a requested high-level credential and return the marshaled  
19 credential to the UTCL.

21           **20. (ORIGINAL)** An architecture as recited in claim 18, wherein

22 the marshaled credentials appear to be a conventional username/password  
23 pair to the UTCL.

421 West Riverside, Suite 500  
Spokane, WA 99201  
P: 509.324-9256  
F: 509.323-8879  
[www.leehayes.com](http://www.leehayes.com)

**lee&hayes**

1           **21. (ORIGINAL)** A computer-readable medium having computer-  
2 executable instructions that, when executed by a computer, employ an  
3 architecture as recited in claim 18.

4  
5           **22. (ORIGINAL)** An operating system embodied on a computer-  
6 readable medium having computer-executable instructions that, when  
7 executed by a computer, employ an architecture as recited in claim 18.

8  
9           **23. (CURRENTLY AMENDED)** An apparatus comprising:

10           a processor;

11           a marshaler executable on the processor to:

12                 obtain a high-level credential, wherein a high-level credential  
13                 is employed in an authorization model which is not username-and-  
14                 password based authorization;

15                 convert the high-level credential to generate a representation  
16                 of the high-level credential that is formatted as a low-level credential  
17                 so that it appears to be a conventional username/password pair.

421 West Riverside, Suite 500  
Spokane, WA 99201  
P: 509.324-9256  
F: 509.323-8979  
[www.leehayes.com](http://www.leehayes.com)

**lee&hayes**

1           **24. (CURRENTLY AMENDED)** A low-level-credential-application  
2 accommodation system comprising:

3           a request obtainer configured to obtain a request for a high-level  
4 credential from a low-level-credential-application, wherein low-level  
5 credentials utilizes username-and-password based authorization while high-  
6 level credentials do not employ username-and-password based  
7 authorization;

8           a credential retriever configured to retrieve the requested credential  
9 from a database of credentials;

10          a marshaller configured to marshal the requested credential and  
11 return the marshaled credential to the low-level-credential-application, the  
12 marshalling performed by the marshaller is characterized by converting a  
13 description of the high-level credential into a format recognizable as a low-  
14 level credential by the low-level-credential-application employing a low-  
15 level credential authorization model.

16  
17          **25. (ORIGINAL)** A system as recited in claim 24, wherein a high-  
18 level credential is a credential selected from a group composed of X.509  
19 Certificates and bio-metrics.

20  
21          **26. (ORIGINAL)** A system as recited in claim 24, wherein the  
22 marshaled credentials appear to be a conventional username/password pair  
23 to the legacy application.

1           **27. (CANCELLED)**

2  
3           **28. (CURRENTLY AMENDED)** A system as recited in claim 24,  
4 wherein the ~~legacy application~~ low-level-credential-application never has  
5 access to the high-level credential.

6  
7           **29. (CURRENTLY AMENDED)** A system for authenticating a user  
8 to a network, the system comprising:

9           a request obtainer configured to obtain a request for a high-level  
10 credential to authenticate the user to access a resource within the network,  
11 wherein the resource requires an appropriate credential before the user may  
12 access the resource, wherein a high-level credential do not utilize  
13 username-and-password based for high-level credential authorization;

14           a credential retriever configured to retrieve the appropriate high-  
15 level credential from a database of credentials;

16           a credential marshaller configured to generate a representation of the  
17 high-level credential that is formatted as a low-level credential so that it  
18 appears to be a conventional username/password pair, wherein a low-level  
19 credential utilizes username-and-password based authorization;

20           a credential returner configured to return the marshaled credential to  
21 the resource within the network, so that the resource allows the user to  
22 access such resource;

23           wherein the obtainer, retriever, marshaller, and returner are further  
24 configured to operate without user interaction.

1           **30. (ORIGINAL)** An operating system comprising a system as  
2 recited in claim 29.

3  
4           **31. (ORIGINAL)** A network environment comprising a system as  
5 recited in claim 29.

6  
7           **32. (ORIGINAL)** An application programming interface (API)  
8 method comprising:

9           receiving a CredUI-promptfor-credentials call having a set of  
10 parameters comprising a TargetName, Context, AuthFlags, and Flags;

11           parsing the call to retrieve the parameters to determine a specified  
12 resource;

13           obtaining a credential;

14           associating the credential with the specified resource;

15           persisting the credential into a database while maintaining the  
16 credential's association with the specified resource.

17  
18           **33. (ORIGINAL)** A method as recited in claim 32, wherein the set  
19 of parameters further comprises an indicator of a data structure containing  
20 customized information to display in conjunction with a user interface.

21  
22           **34. (ORIGINAL)** An application programming interface (API)  
23 method comprising:

24           receiving a CredUI-promptfor-credentials call having a set of  
25 parameters comprising a TargetName, UserName, Password, and Flags;

1        parsing the call to retrieve the parameters to determine a requesting  
2 application;

3        obtaining a low-level credential from a user, wherein such credential  
4 includes a username and a password;

5        returning the low-level credential to the requesting application.

6

7        **35. (ORIGINAL)** A method as recited in claim 34, wherein the set  
8 of parameters further comprises an indicator of a data structure containing  
9 customized information to display in conjunction with a user interface.

421 West Riverside, Suite 500  
Spokane, WA 99201  
P: 509.324.9256  
F: 509.323-8979  
www.leehayes.com

**lee&hayes**